Content management serves as a vital cyberspace operations enabler

By Russell Fenton

The importance of cyberspace, as part of the nation's critical infrastructure, arose from the President's signing of the National Strategy to Secure Cyberspace in February of 2003. Since then, many important national strategies, policies, and decisions have been created and signed. Consequently, the Department of Defense created the National Military Strategy for Cyberspace Operations in December 2006, and subsequent NMS-CO Implementation Plan in October 2007.

Although cyberspace has been defined in many different ways within private and public communities over the years, on 12 May 08, the Under Secretary of Defense, Gordon England, signed a document officially establishing the DoD definition:

Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Along with the cyberspace definition, the chairman of the Joint Chiefs of Staff approved the definition of Cyberspace Operations in August 2009: [Cyberspace Operations are] the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.

For decades, the Army has used its portion of cyberspace (the LandWarNet) and cyberspace operations to enable a continuing strategic, operational, and tactical information advantage over adversaries of the U.S; yet the advent of the official cyberspace definition, as well as recent national defense strategies, elevates cyberspace to the same level as land, sea, air, and space. Ultimately, this creates a paradigm shift because we must now think of the network as a virtual area of operations where the information modified, stored, and exchanged within it is more than just integrated data with a higher meaning. Information has now transitioned to a tool that can create non-kinetic effects in and through cyberspace. So the question must be asked, "Are content management capabilities (with the goal of getting the right information to the right place, at the right time, and in the right format) a vital enabler to cyberspace operations?" While some will undoubtedly argue the point, as the rest of this article will attempt to explain, the answer is "yes."

Recognizing and fully understanding the cyberspace domain is the first step in appreciating how content management enables cyberspace operations. Cyberspace has characteristics that differ significantly from the land, air, sea, and space domains. Figure 1 depicts cyberspace as consisting of three layers (physical, logical, and social) made up of five components (geographic, physical network, logical network, cyber persona, and persona).

The physical layer includes the geographic component and the physical network component. The geographic component is the physical location of elements of the network. While you can easily cross geographical boundaries in cyberspace at a rate approaching the speed of light, there is still a physical aspect tied to the other domains. The physical network component includes all of the hardware and infrastructure (wired, wireless, and optical) that supports the network and the physical connectors (wires, cables, radio frequency, routers, servers, and computers).

The logical layer contains the logical network component, which is technical in nature and consists of the logical connections that exist between network nodes. Nodes are any devices connected to a computer network. Nodes can be computers, personal digital assistants, cell phones, or various other network appliances. On an Internet protocol network, a node is any device with an IP address.

The social layer comprises the human and cognitive aspects and includes the persona component and the cyber persona component. The cyber persona component includes a person's identification or persona on the network (e-mail address, computer IP address, cell phone number, and others). The persona component consists of the people actually on the network. An individual can have multiple cyber personas (for example, different e-mail accounts on different computers) and a single cyber persona can have multiple users (for example, multiple users accessing a single Facebook account). The social layer is primarily application based, and it is concerned with how users and information systems present, store, and modify information. Meaningful interaction and function

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Content management serves as a vital cyberspace operations enabler	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Signal Center,ATTN: ATZH-POM (Army Communicator),Bldg 29808A (Signal Towers), Room 713,Fort Gordon,GA,30905**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**3**	

through cyberspace occurs when all three layers are integrated and operating correctly.

Another step in appreciating how CM is an enabler to cyberspace operations is understanding how information has become a force in its own right. As stated in FM 3-0, "Information is a powerful tool in the operational environment. In modern conflict, information has become as important as lethal action in determining the outcome of operations." In the physical realm, every engagement, battle, and major operation requires complementary information to both inform and influence audiences within the operational area. It is an element of combat power against enemy command and control and it is a means to affect enemy morale. It is both destructive and constructive.

Given the transitioning view of cyberspace as a domain, one must consider that information within the virtual realm can be fired from a weapons platform in order to create desired effects. If information is part of a weapon, and the aim of the information weapon is to achieve objectives in cyberspace, then what is the target? The answer varies depending on whom you ask. Some will say information itself is a lucrative target. Others say the focal point is on the cognitive level and how information can influence the adversary or win the hearts and minds of the people. Still others say utilize information to deny, disrupt, or degrade adversary command and control systems (e.g. denial of service attack).

In the end, the network is a weapon platform. The information on the network is analogous to munitions or forces on the battlefield, and the non-kinetic effects created can be just as powerful as any kinetic weapon in our arsenal.

This all begs the question, "How does CM act as a vital enabler to operations in the cyberspace domain?" FM 6-02.71 (Network Operations) explains how CM utilizes technologies, techniques, processes, policies, and procedures necessary to assure the delivery of information. CM relies on the physical and logical layers of cyberspace in order to move and maneuver information within the virtual area of operations to ensure information time on target in the social layer of cyberspace. This process is the equivalent of forces maneuvering to gain positions of advantage in the traditional land domain. As stated before, cyberspace operations involve the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through the domain. For CM, the objective in and through cyberspace is to deliver the right information to the right place, at the right time, and in the right format to create the necessary effects.

To move and maneuver content as part of cyberspace operations, several functions must be performed.

First, information must be assembled and held for onward movement. These assembly areas in cyberspace consist of technologies such as network access storage and temporary caching.

Second, resources must be allocated based on the

(Continued on page 24)

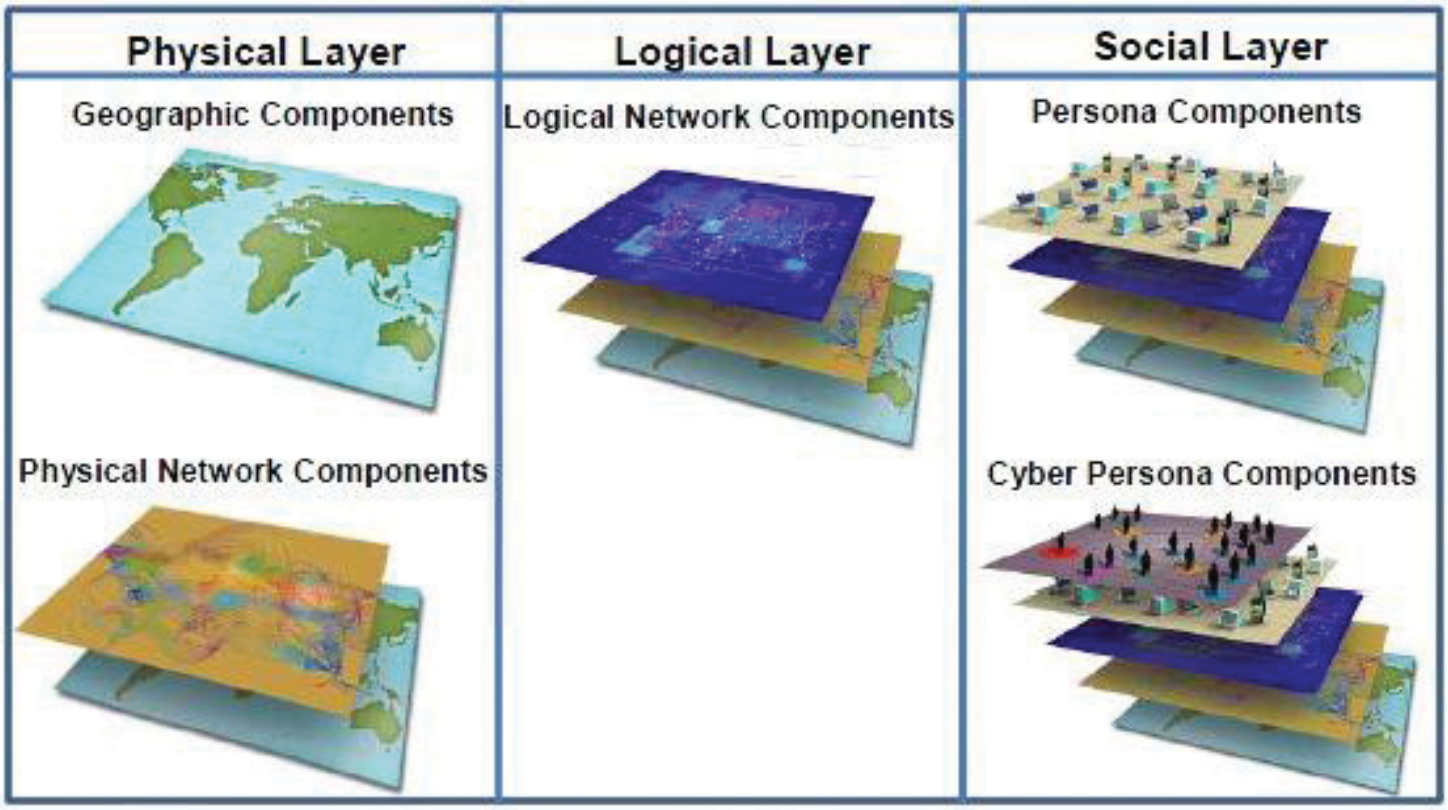

Figure 1

(Continued from page 23)

commander's priorities and to balance requirements against capabilities. Individuals need to plan for the known and posture anticipatory measures for the unknown. In certain events, rapid response is required to meet emergencies and support unexpected opportunities. Frequent movement of information using transport and staging capabilities normally committed to other tasks makes maintaining continuity of operations support a challenge.

Third, network operators will manage and direct information movement on main routes and alternate network routes, and maneuver information around areas of degradation or disruption.

Fourth, network operators must coordinate with warfighters in order to match requirements with methods based on priorities, the principles of movement control, and the capabilities selection guidelines.

Lastly, information movement and maneuver must be tracked (in-transit visibility) from origin to destination. ITV provides situational awareness of information flow within the virtual area of operations.

The U.S. Army Training and Doctrine Command has recognized the importance of determining capabilities that commanders must bring bear to enable Army Cyberspace Operations. In February 2010, TRADOC published TRADOC Pamphlet 525-7-8 (Army Cyberspace Operations Concept Capability Plan). This publication describes how the Army will fight and win the cyber/electromagnetic contest, focusing on the timeframe of 2016 – 2028. In order for the Army to prevail, it must gain the advantage, protect this advantage, and place the adversary at a disadvantage in cyberspace. Per the CCP, the components of Army Cyberspace Operations consist of Cyberspace Situational Awareness, Cyberspace Warfare, Cyberspace Support, and Network Operations. CM is the function within NetOps that enables commanders to gain an information advantage over the adversary.

At some point, all CM activities conducted in cyberspace must facilitate land operations. Remember, it is the social layer of cyberspace that integrates with the cognitive aspects of the information environment. The information that exists at this layer is meaningful to humans or connected devices and ultimately informs, influences, or facilitates understanding and decision-making.

As part of land operations, both knowledge management and inform and influence activities rely on the management of content in cyberspace. KM is the art of creating, organizing, applying, and transferring knowledge to facilitate situational understanding and decision-making; while, IIA are conducted to inform domestic audiences and influence foreign friendly, neutral, adversary, and enemy audiences. Field Manual (FM) 6-01.1 (Knowledge Management Section) and Change 1 of FM 3-0 (Operations) highlight CM's role in supporting KM and IIA respectively.

For decades the Army has used its portion of cyberspace (the LandWarNet) and cyberspace operations to enable a continuing strategic, operational, and tactical information advantage over adversaries. Yet, the emergence of cyberspace as a domain and the thought of conducting operations in it versus just through it that has forced a paradigm shift in which the network has become a weapons platform and the information within it acts as munitions that can be fired or forces that can be moved and maneuvered on the virtual battlefield.

CM leverages the physical and logical layers of cyberspace for the purposes of staging information, allocating cyberspace assets, routing, and in-transit visibility, with the end objective of delivering the right information to the right place, at the right time, and in the right format within the social layer. Undoubtedly, CM is a vital enabler to cyberspace operations that supports operations in the land domain and sets the conditions for the Army to prevail in the cyber/electromagnetic contest.

Russell Fenton *is a retired Signal (25A) and information systems management officer (FA53A) with over 17 years network operations experiences at all echelons. Mr. Fenton currently works as the Chief of the Cyberspace Cell, Network Assurance Section, TRADOC Capabilities Management Office Global Network Enterprise, U.S. Army Signal Center of Excellence. He has spent the last three years working as part of the Army integrated capabilities development team developing the capstone concept and identifying network operations solutions in support of cyberspace operations.*

Acronym QuickScan

CCP - Concept Capability Plan
CM - Content Management
DoD - Department of Defense
IIA - Inform Influence Activities
IP - Internet Protocol
IT - Information Technology
ITV - In Transit Visibility
KM - Knowledge Management
NetOPS - Network Operations
NMS-CO - National Military Strategy Cyberspace Operations
TRADOC - U.S. Army Training and Doctrine Command